ABSTRACT

An electronic asset system mints a stick of electronic assets that can be spent by the user with multiple vendors. Assets sticks are issued anonymously or non-anonymously in a way without requiring dedication to a particular vendor, hence allowing the user to spend one or more assets from the stick with different vendors. The auditor randomly audit samples of the spent assets to detect whether the assets have been fraudulently used. The electronic asset system employs tamper-resistant electronic wallets constructed as dedicated hardware devices, or as devices with secure-processor architecture. The electronic asset system also facilitates handling of electronic coupons in a manner that enforces compliance between the user and the vendor. The user and vendor each maintain a stick of corresponding coupons with pointers to the most recent and oldest coupons available for expenditure. When a coupon is used or granted, the user and vendor both update the appropriate pointer to their respective sticks and then exchange signed data describing placement of the pointer to verify a correspondence between the referenced coupons.